WHAT IS CLAIMED IS:

1. A method of generating key information, comprising the steps of:

rearranging bits of a first bit sequence in a first matrix according to a predetermined arrangement rule, the first bit sequence representing information being a base of a key;

forming blocks in the first matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the first matrix;

executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation;

combining the logical-operation-result bits into a second bit sequence, wherein the number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence; and

accessing a second matrix composed of predetermined third bit sequences and reading out one from among the third bit sequences in response to the second bit sequence, and outputting the read-out third bit sequence as information representative of the key, wherein the number of bits composing each of the third bit sequences is smaller than the number of bits composing the second bit sequence.

2. An apparatus for generating key information, comprising:

means for rearranging bits of a first bit sequence in a first matrix according to a predetermined arrangement rule, the first bit sequence representing information being a base of a key;

means for forming blocks in the first matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the first matrix;

means for executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation;

means for combining the logical-operation-result bits into a second bit sequence, wherein the number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence; and

means for accessing a second matrix composed of predetermined third bit sequences and reading out one from among the third bit sequences in response to the second bit sequence, and outputting the read-out third bit sequence as information representative of the key, wherein the number of bits composing each of the third bit sequences is smaller than the number of bits composing the second bit sequence.

3. A method of encrypting contents information, comprising the steps of:

generating a signal representative of a key from information being a base of the key, the key base information including a first bit sequence; and

encrypting contents information in response to the key signal;

wherein the generating step comprises:

1) rearranging bits of the first bit sequence in a first matrix according to a predetermined arrangement rule;

2) forming blocks in the first matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the first matrix;

3) executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation;

4) combining the logical-operation-result bits into a second bit sequence, wherein the number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence; and

5) accessing a second matrix composed of predetermined third bit sequences and reading out one from among the third bit sequences in response to the second bit sequence, and outputting the read-out third bit sequence as the key signal, wherein the number of bits composing each of the third bit sequences is smaller than the number of bits composing the second bit sequence.

4. An apparatus for encrypting contents information, comprising:

means for generating a signal representative of a key from information being a base of the key, the key base information including a first bit sequence; and

means for encrypting contents information in response to the key signal;

wherein the generating means comprises:

1) means for rearranging bits of the first bit sequence in a first matrix according to a predetermined arrangement rule;

2) means for forming blocks in the first matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the first matrix;

3) means for executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation;

4) means for combining the logical-operation-result bits into a second bit sequence, wherein the number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence; and

5) means for accessing a second matrix composed of predetermined third bit sequences and reading out one from among the third bit sequences in response to the second bit sequence, and outputting the read-out third bit sequence as the key signal, wherein the number of bits composing each of the third bit sequences is smaller than the number of bits composing the second bit sequence.

5. A method of decrypting contents information, comprising the steps of:

generating a signal representative of a key from information being a base of the key, the key base information including a first bit sequence; and

decrypting encryption-resultant contents information in response to the key signal;

wherein the generating step comprises:

1) rearranging bits of the first bit sequence in a first matrix according to a predetermined arrangement rule;

2) forming blocks in the first matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the first matrix;

3) executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation;

4) combining the logical-operation-result bits into a second bit sequence, wherein the number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence; and

5) accessing a second matrix composed of predetermined third bit sequences and reading out one from among the third bit sequences in response to the second bit sequence, and outputting the read-out third bit sequence as the key signal, wherein the number of bits composing each of the third bit sequences is smaller than the number of bits composing the second bit sequence.

6. An apparatus for decrypting contents information, comprising:

means for generating a signal representative of a key from information being a base of the key, the key base information including a first bit sequence; and

means for decrypting encryption-resultant contents information in response to the key signal;

wherein the generating means comprises:

1) means for rearranging bits of the first bit sequence in a first matrix according to a predetermined arrangement rule;

2) means for forming blocks in the first matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the first matrix;

3) means for executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation;

4) means for combining the logical-operation-result bits into a second bit sequence, wherein the number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence; and

5) means for accessing a second matrix composed of predetermined third bit sequences and reading out one from among the third bit sequences in response to the second bit sequence, and outputting the read-out third bit sequence as the key signal, wherein the number of bits composing each of the third bit sequences is smaller than the number of bits composing the second bit sequence.

7. A recording medium storing encryption-resultant key base information and encryption-resultant contents information generated by the method in claim 3.

8. A method of transmitting contents information, comprising

the steps of transmitting encryption-resultant key base information through a transmission line, and transmitting encryption-resultant contents information through the transmission line, the encryption-resultant contents information being generated by the method in claim 3.

9. A method of generating key information, comprising the steps of:

dividing a first bit sequence into second bit sequences, the first bit sequence being contained in information being a base of a key, wherein the number of bits composing each of the second bit sequences is smaller than the number of bits composing the first bit sequence;

sequentially accessing a first matrix composed of predetermined data pieces and sequentially reading out ones from among the predetermined data pieces in response to the second bit sequences;

combining the read-out data pieces into a third bit sequence, wherein the number of bits composing the third bit sequence is smaller than the number of bits composing the first bit sequence;

rearranging bits of at least part of the third bit sequence in a second matrix according to a predetermined arrangement rule;

forming blocks in the second matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the second matrix;

executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation; and

combining the logical-operation-result bits into a fourth bit sequence, and outputting the fourth bit sequence as at least part of information representative of the key, wherein the number of bits composing the fourth bit sequence is smaller than the number of bits composing the second matrix.

10. An apparatus for generating key information, comprising:

means for dividing a first bit sequence into second bit sequences, the first bit sequence being contained in information being a base of a key, wherein the number of bits composing each of the second bit sequences is smaller than the number of bits composing the first bit sequence;

means for sequentially accessing a first matrix composed of predetermined data pieces and sequentially reading out ones from among the predetermined data pieces in response to the second bit sequences;

means for combining the read-out data pieces into a third bit sequence, wherein the number of bits composing the third bit sequence is smaller than the number of bits composing the first bit sequence;

means for rearranging bits of at least part of the third bit sequence in a second matrix according to a predetermined arrangement rule;

means for forming blocks in the second matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the second matrix;

means for executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation; and

means for combining the logical-operation-result bits into a fourth bit sequence, and outputting the fourth bit sequence as at least part of information representative of the key, wherein the number of bits composing the fourth bit sequence is smaller than the number of bits composing the second matrix.

11. A method of encrypting contents information, comprising the steps of:

generating a signal representative of a key from information being a base of the key, the key base information including a first bit sequence; and

encrypting contents information in response to the key signal;

wherein the generating step comprises:

1) dividing the first bit sequence into second bit sequences, wherein the number of bits composing each of the second bit sequences is smaller than the number of bits composing the first bit sequence;

2) sequentially accessing a first matrix composed of predetermined data pieces and sequentially reading out ones from among the predetermined data pieces in response to the second bit sequences;

3) combining the read-out data pieces into a third bit

sequence, wherein the number of bits composing the third bit sequence is smaller than the number of bits composing the first bit sequence;

4) rearranging bits of at least part of the third bit sequence in a second matrix according to a predetermined arrangement rule;

5) forming blocks in the second matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the second matrix;

6) executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation; and

7) combining the logical-operation-result bits into a fourth bit sequence, and outputting the fourth bit sequence as at least part of the key signal.

12. An apparatus for encrypting contents information, comprising:

means for generating a signal representative of a key from information being a base of the key, the key base information including a first bit sequence; and

means for encrypting contents information in response to the key signal;

wherein the generating means comprises:

1) means for dividing the first bit sequence into second bit sequences, wherein the number of bits composing each of the second bit sequences is smaller than the number of bits composing the first bit sequence;

2) means for sequentially accessing a first matrix composed of

predetermined data pieces and sequentially reading out ones from among the predetermined data pieces in response to the second bit sequences;

3) means for combining the read-out data pieces into a third bit sequence, wherein the number of bits composing the third bit sequence is smaller than the number of bits composing the first bit sequence;

4) means for rearranging bits of at least part of the third bit sequence in a second matrix according to a predetermined arrangement rule;

5) means for forming blocks in the second matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the second matrix;

6) means for executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation; and

7) means for combining the logical-operation-result bits into a fourth bit sequence, and outputting the fourth bit sequence as at least part of the key signal.

13. A method of decrypting contents information, comprising the steps of:

generating a signal representative of a key from information being a base of the key, the key base information including a first bit sequence; and

decrypting encryption-resultant contents information in response to the key signal;

wherein the generating step comprises:

1) dividing the first bit sequence into second bit sequences, wherein the number of bits composing each of the second bit sequences is smaller than the number of bits composing the first bit sequence;

2) sequentially accessing a first matrix composed of predetermined data pieces and sequentially reading out ones from among the predetermined data pieces in response to the second bit sequences;

3) combining the read-out data pieces into a third bit sequence, wherein the number of bits composing the third bit sequence is smaller than the number of bits composing the first bit sequence;

4) rearranging bits of at least part of the third bit sequence in a second matrix according to a predetermined arrangement rule;

5) forming blocks in the second matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the second matrix;

6) executing logical operation among bits in each of the blocks and generating a bit being a result of the logical operation; and

7) combining the logical-operation-result bits into a fourth bit sequence, and outputting the fourth bit sequence as at least part of the key signal.

14. An apparatus for decrypting contents information, comprising:

means for generating a signal representative of a key from information being a base of the key, the key base information including a first bit sequence; and

means for decrypting encryption-resultant contents information in response to the key signal;

wherein the generating means comprises:

1) means for dividing the first bit sequence into second bit sequences, wherein the number of bits composing each of the second bit sequences is smaller than the number of bits composing the first bit sequence;

2) means for sequentially accessing a first matrix composed of predetermined data pieces and sequentially reading out ones from among the predetermined data pieces in response to the second bit sequences;

3) means for combining the read-out data pieces into a third bit sequence, wherein the number of bits composing the third bit sequence is smaller than the number of bits composing the first bit sequence;

4) means for rearranging bits of at least part of the third bit sequence in a second matrix according to a predetermined arrangement rule;

5) means for forming blocks in the second matrix, wherein each of the blocks has bits, the number of which is smaller than the number of bits composing the second matrix;

6) means for executing logical operation among bits in each of the blocks and generating a bit being a result of the logical

operation; and

7) means for combining the logical-operation-result bits into a fourth bit sequence, and outputting the fourth bit sequence as at least part of the key signal.

15. A recording medium storing encryption-resultant key base information and encryption-resultant contents information generated by the method in claim 11.

16. A method of transmitting contents information, comprising the steps of transmitting encryption-resultant key base information through a transmission line, and transmitting encryption-resultant contents information through the transmission line, the encryption-resultant contents information being generated by the method in claim 11.